

Reflexiones sobre el Esquema Nacional de Seguridad

El Esquema Nacional de Seguridad es la plasmación de lo que ya se anticipaba en el artículo 42 de la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (Ley 11): la creación de unas políticas de seguridad comunes en las Administraciones Públicas. Tiene como objetivo, por la parte de los usuarios finales, la generación de la confianza de los ciudadanos en el uso de los medios de acceso electrónico, que se ponen a su alcance bajo la Ley 11, y, por parte de las Administraciones Públicas, el fomento de la confianza en los procesos de cooperación en los servicios proporcionados a los ciudadanos, y el permitir, en el momento de alcanzar todos los involucrados la conformidad con el ENS, la consecución de un nivel común de seguridad y protección de los datos.

POR JAVIER BUSTILLO

Los principios básicos del ENS presentan una gestión de la seguridad moderna, basada en aportaciones de múltiples fuentes españolas y europeas, que normalmente se reflejan bajo el Plan Director de Seguridad con puntos importantes para garantizar una seguridad integral y transversal a todos los servicios, entre los que cabe destacar los siguientes:

- * La definición de la seguridad como una función diferenciada de la gestión y operación de los sistemas, segregando la responsabilidad de la seguridad en un Gestor de seguridad.

- * La integración de seguridad física y lógica para alcanzar una gestión global de la seguridad.

- * La definición de las políticas ba-



Abre un abanico de nuevas oportunidades para consolidar la gestión de la seguridad de las Administraciones Públicas, bajo unos criterios comunes que contribuyan a garantizar el servicio que los ciudadanos demandan

sadas en una evaluación de los riesgos y su posible impacto en los servicios, lo que permitirá priorizar de manera correcta las inversiones.

* La supervisión, no sólo de los sistemas y comunicaciones, sino también de las personas y proveedores involucrados en los procesos.

* La definición de unos requisitos mínimos a cumplir por todas las administraciones en cada uno de los puntos de control, de forma que se cree un mínimo común a cumplir que se pueda medir.

* Un proceso de auditoría bianual de mejora continua, que servirá para mostrar a los usuarios y demás Administraciones que se está conforme a las exigencias del ENS.

Hay varios puntos de los requisitos mínimos que también exigirán por parte de los socios tecnológicos un compromiso de cara a colaborar con las Administraciones Públicas para cumplir el ENS:

* El Artículo 18 (adquisición de productos de seguridad) hace una expresa petición de que las soluciones estén certificadas bajo los mejores estándares de seguridad a nivel nacional e internacional. Esto requerirá contar con colaboradores tecnológicos que como EMC, a través de nuestra división de seguridad (RSA), sean capaces de comprometerse a continuar invirtiendo en I+D para que sus soluciones de seguridad estén certificadas bajo estándares reconocidos, como "Common Criteria".

* El Artículo 21 (protección de información almacenada y en tránsito), se refiere a un ámbito donde EMC (RSA) cuenta con experiencia en diferentes organismos de la Administración Pública, con los que ha colaborado en proyectos para proporcionar protección y cifrado de datos

en todos los puntos de utilización y almacenamiento de la información, y extensible a todos los puntos donde se utilicen datos confidenciales. Los socios tecnológicos tendremos que continuar la expansión de la utilización de un Gestor Corporativo de Claves que sea capaz de integrarse con un mayor número tecnologías y aplicaciones a medida que se extienda su uso.

* Artículo 23 (registro de actividad). Uno de los pilares de la seguridad para la Administración es tener un sistema capaz de almacenar todas las actividades de usuarios, administradores, cambios de configuración y de permisos que den acceso a información confidencial, de manera que los datos estén asegurados para su disponibilidad en el futuro ante la necesidad de demostrar cualquier actividad anómala. Estos sistemas seguirán exigiendo cada vez mejores y más fáciles integraciones con sistemas de cada vez mayor número de fabricantes, lo que se ha demostrado con la explosión de las instalaciones de soluciones SIEM (Security Information and Event Management) en los últimos años en España, que ha provocado la integración de múltiples dispositivos nuevos, presentes en las instalaciones de nuestros clientes.

* Artículo 25 (continuidad de la actividad). Los proveedores tendremos que proporcionar no sólo sistemas de back-up, sino sistemas que faciliten la mejor recuperación para asegurar la continuidad de negocio y la recuperación de la operativa en el plazo más corto posible. De la misma manera, tendremos que colaborar con los responsables de seguridad de los distintos organismos de la Administración en la definición de Planes

FIGURA 1. Diferentes grupos de gestión



de Recuperación ante Desastres, que contemplen todos los sistemas regulados bajo el ENS.

Uno de los puntos más interesantes del ENS es la definición del modelo de gestión de la seguridad que plantea. Al estar basado en los trabajos de normalización de los principios de gestión de seguridad, está muy alineado con los sistemas modernos de e-GRC (Enterprise Governance, Risk and Compliance), como RSA Archer, que se enfocan en el control de todos los aspectos de la seguridad, desde el punto de vista del gestor corporativo de seguridad, al cual proporcionan, en todo momento, una visión global de la situación de cada uno de los procesos que están involucrados en la gestión de las políticas. Estos sistemas integran en un solo repositorio la gestión del

estado de los riesgos identificados, las políticas definidas para paliarlos, la capacitación del personal asignado, los proveedores, los incidentes y sus respuestas, y las auditorías periódicas, pudiendo representar una herramienta clave para medir y controlar de forma continua el estado de conformidad con el ENS.

Como podemos ver, el ENS abre un abanico de nuevas oportunidades para consolidar la gestión de la seguridad de las Administraciones Públicas, bajo unos criterios comunes que contribuyan a garantizar el servicio que los ciudadanos demandan. Evidentemente, la celeridad en la incorporación de este tipo de tecnologías vendrá marcada por varios factores exógenos y endógenos a este proceso: la percepción del usuario final, el ciudadano, de que las transacciones

que realiza cumplen con los requisitos de privacidad establecidos; el desarrollo continuo del marco legislativo que permita proteger los intereses de los ciudadanos cuando deleguen la salvaguarda de su “vida electrónica” a terceros; y, finalmente, el apoyo presupuestario necesario para el impulso de este tipo de soluciones tecnológicas, como prioritarias en los entornos que salvaguardan y gestionan transacciones con información sensible de los ciudadanos. 🌹